Sophia University
Information Security Handbook (ver.1.5)
(Proposed)

Information and Communication Technology is progressing rapidly in the fields of education and research as well, and the use of computers and the Internet is increasing. At the same time, threats on the Internet are also increasing. Examples of this include the exploiting of information and communications technology spreading computer viruses and the sending of massive amounts of spam and fraudulent mails. Our university has also faced serious security incidents, including virus infection and account hacking that could lead to information leak incidents.

Please use this handbook to understand the necessity of information security measures and to implement countermeasures.

November 1, 2019

ICT Office, Sophia University

Document 6

Information Security Policy: 18 Steps

1. Software Vulnerability Measures (OS, Office applications, etc.)
2. Antivirus Measures for Computers
3. Security Measures for Wireless LAN
4. Policies for Using File Sharing and Other Software
5. Password Management
6. Managing Access to Sensitive Information
7. Measures against Targeted Attack Email
8. Measures against Misdirected Email
9. Preventing Information Leak through Email
10. Avoiding Internet Trouble (SNS, etc.)
11. Preventing Unauthorized Use of Online Services
12. Backing Up Sensitive Information
13. Managing Important Computing Equipment
14. Physically Protecting Sensitive Information
15. Managing Sensitive Information Used Off Campus
16. Procedures for Disposing of Unneeded Computers
17. Proper Software Management
18. Server Room Management

STEP

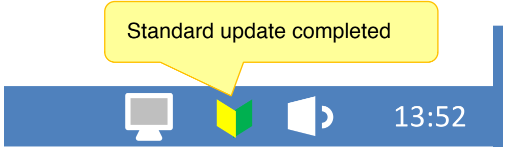
01

Software Vulnerability Measures (OS, Office applications, etc.)

Over time, web browsers, e-mail software, OS, Office applications, and other software may encounter a problem called vulnerability. If you fail to solve the vulnerability problem, even if you install antivirus software, there is a high risk of virus infection or of intrusion from another computer. Please be sure to take the following precautionary measures against software vulnerability:

□ Update OS and software regularly.

On Windows, using Windows Update will strengthen protection against vulnerability (The weak point in a program where viruses can easily enter).



Standard update completed

13:52

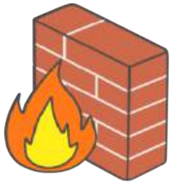
□ On other OS and software, determine how to update and do so regularly.

□ As much as possible, do not use OS or software that is no longer supported.

- If there are no alternatives, take measures such as not connecting to the network.
- Windows 7 will continue being supported until January 2020.

□ When a firewall is being used as standard on PCs and other devices, make sure the appropriate settings are used.

A firewall functions to controls the communication between the PC's network and the Internet.



STEP

02

Antivirus Measures for Computers

Recent viruses are becoming diverse and sophisticated and are able to do such things as display e-mails, or infect websites merely by browsing them with web browsers. Also, compared to the past, some attacks work in such a way that the contents and magnitude of the damage are not immediately detected. In addition, virus infection claims its next victim not only by the first target's information leakage but also through secondary and tertiary infections, so there is also the danger of unknowingly becoming a perpetrator.

□ **Install antivirus software**.
(Available from the ICT Office:
https://ccweb.cc.sophia.ac.jp/userguide/service/sv_01/)

□ **Automatically update** anti-virus software **definition file**.
Simply installing antivirus software will not allow it to always respond to the latest virus. It is necessary to always keep the pattern file up-to-date.

□ **Run virus scan on a regular basis**.

□ **Confirm cases of damage** due to virus infection inside and outside the university.

□ Regularly take part in **security workshops**.

The ICT systems manager will explain the types of viruses prevalent and the route they take to infect systems.

□ Do not use **storage media** that is not permitted or whose owner is unknown.

□ When you insert storage media, be sure to run a virus check before opening folders and files.

There are incidents in which a virus is spread just by inserting storage media such a USB memory into a personal computer and using the automatic execution function.

STEP 03

Security Measures for Wireless LAN

Wireless LAN is also being introduced in homes and offices because of its high convenience. Recently, public wireless LAN service has become widespread, and it is now available in stations, airports, cafes and restaurants as well. However, because wireless LAN communicates using radio waves, there is a danger of others stealing communication contents.

Also, when installing wireless a LAN router you purchased yourself at home, in your office, or elsewhere, please pay attention to the security settings.

□ Use only university-recommend wireless LAN devices. Sophia University designated LAN: **Sophia Wi-Fi**

□ Public wireless LAN is not used for business or research because its safety cannot be guaranteed.

Wireless LAN Risks

Public wireless LAN service have become popular in hotels and restaurants, and places where wireless LAN is available have increased. Especially for wireless LANs that do not require input of passwords, etc., or for wireless LANs that can be used with common passwords, be careful to confirm their reliability before accessing.

Wireless LAN has become easy to use, with wireless LAN routers purchased for individual use at home or in an office, or mobile routers rented when traveling abroad. While these devices are convenient and easy to use, please use the following functions to enhance safety (examples given for reference).

◆A fixed number called a MAC address is assigned to the communication device. When configuring the router, register the MAC address and limit the clients that can use it.

◆ The wireless LAN router has a name (SSID) to identify it, and an encryption key (password). Although it is possible to use the initial password as it is, change the name to strengthen the security and do not use the name of the user or organization, etc. which is easy to guess.

STEP

04

Policies for Using File Sharing and Other Software

When file sharing software is used, there is the risk of virus infection. Such infection could result in leakage of research, class and personal information stored on personal computers and other devices to the network. Information leakage can lead to claims for compensation for damages and both emotional and economic difficulties.

Please take the following measures for using software:

□ **Do not use file sharing software intended for use by an unspecified number of people.**

□ **Only use software purchased from a legitimate provider.**

□ Use an external (Cloud) service with contract terms.

File Sharing Software

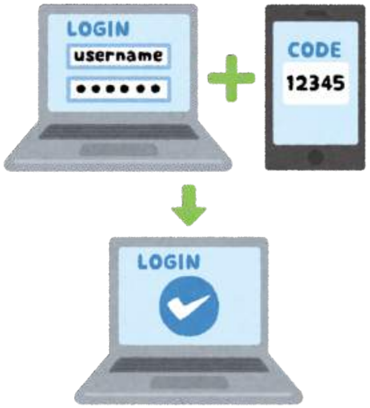
File sharing software allows unspecified users to share files on the Internet. Many file sharing software such as "Winny" have existed in Japan, but much of the sharing of music, movies, television programs, game software and other data done through such software violated copyright law, making this a social problem. Viruses targeting file sharing software have resulted in many incidents of leakage on the Internet of confidential information of companies and organizations. As much as possible, avoid using file sharing software.

Since we are using Sophia Mail, we recommend OneDrive provided with Office 365.
How to use OneDrive:
https://ccweb.cc.sophia.ac.jp/documents/#_217

STEP

05

Password Management



It is important to create a secure password that is hard to guess and keep it appropriately so that it will not be seen by others, so that others cannot use your account illegally.

Please practice password management as follows:

□ Do not use personal information such as name or birthdate.

□ Use 8 or more characters including alphanumeric characters.

- Combinations of upper and lowercase letters, numbers, and symbols are desirable.
- When there is a system restriction, make it as close to the above as possible.

□ Write the password on paper; do not put in on your desktop.

□ Do not carelessly reveal it to other people.

□ Do not use the same password for multiple services.

□ If a service has 2-step authentication (enter security code along with ID and password), use this procedure.

Making a secure password ●

1. Think of an appropriate password that includes numbers.

Ex: "I am learning Yoga every Wednesday night from 6 o'clock"

2. Follow a rule such as using only the first letter of words or omitting vowels.

"IalyeWnf6o"

3. Use upper and lower case letters; exchange: l＝1·O＝０·a=@, etc.

"I@1yeWnf6o" Completed!

STEP

06

Managing Access to Sensitive Information

When information stored in the equipment connected via a network can be viewed from the Internet (outside the campus), this becomes a problem. In some cases, this leads to information leakage via the Internet or cyberattacks due to the unauthorized use of connected equipment. To control access to important information, please do the following:

- □ When sharing equipment in an office, allow access only on a need-to-know basis.
- □ Do not share the same ID or password.
- □ Be sure to reset initial passwords.

Failure to Take Security Measures

Stepping Stones
When accessing another person's computer, if the hacker connects directly from their own computer, there is a possibility that the hacker be identified by the IP address of the connection source. In order to make it harder to find their computer, hackers go through several computers before connecting to the target computer. A computer used only as a relay point, called a stepping stone, may unknowingly become a perpetrator.

Networked Multifunction Printers:
A computer used as a relay point of unauthorized intrusion.

STEP

07

Measures against Targeted Attack Email

Frequent incidents occur where important information is stolen by targeted attack email aimed at specific companies and organizations. Targeted attack email is a virus that is crafted skillfully so as to lead recipients to believe that the person in charge of the organization, for example, has sent a business-related email. When the recipient opens the email attachment, important information can be stolen.

As a countermeasure against targeted attack email, please observe the following policy:

□Do not open attachments on suspicious emails or click on URLs in the email text.

□Be aware of cases of targeted attack email.

□Regularly take part in Internet security workshops.

Targeted Attack Mail ●

Beware of suspicious mails!

□ Although the content is public, the sender uses free mail.
□ Although the attached file is in exe format or in ZIP (compressed), the file icon is Word, Excel, PDF, etc.
□ Japanese text is unnatural (as though it were automatically translated).
□ *A link in the text leads to another site.

If you mistakenly open a suspicious e-mail attachment or click on a URL in the body of the e-mail, please contact the ICT Office (Media Center).

Contact: Extension <3101> or <4473>

STEP

08

Measures against Misdirected Email

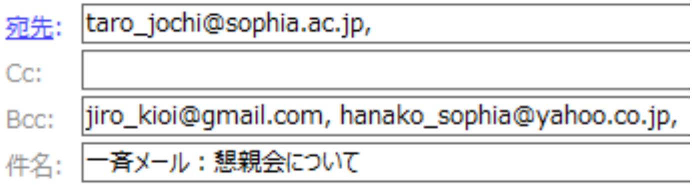
When sending emails, information leaks frequently occur due mistakes in the destination address or incorrect designation of the display method of the mail address (To/Cc/Bcc).

As a countermeasure against erroneous transmission of email, please observe the following:

- □ Confirm mail addresses before sending email.
- □ Be sure to use To, Cc, and Bcc properly.
- □ When sending email to multiple recipients, use the mailing list (ML) prepared by our university to prevent sending errors due to mistakes in recipients' addresses.
- □ （Use the "confirmation dialog" of email software (such as Outlook) that urge confirmation before sending email.

Sending Mail to Multiple Recipients

When sending the same email to multiple recipients, address the mail to yourself and include recipients' addresses in the "Bcc" line. Each recipient will then see your address in the destination line (To). Although ideally all recipients are acquainted, putting all of their addresses in the "To" line makes it all too easy for a stranger to learn recipients' addresses. Be careful not to enter all recipients' addresses in the "To" line.



宛先: taro_jochi@sophia.ac.jp,
Cc:
Bcc: jiro_kioi@gmail.com, hanako_sophia@yahoo.co.jp,
件名: 一斉メール：懇親会について

STEP

09

Preventing Information Leak through Email

Incidents such as information leak have occurred due to the mistaken transmission of an email that has an attached file containing data such as personal information.

To prevent information leak from emails, please observe the following:

- □ When sending an attached file, encrypt the file (with password).
- □ Do not write the password used for encryption in the email to which the file is attached. Communicate the password another way, such as by telephone.
- □ Alternatively, use the file transfer service recommended by the university.

File Sending Services

When attaching a file by email, there is a limit on its size (within the campus network the limit is 10 MB, including the email itself). Generally, "file transfer service" is used when sending and receiving large capacity or large amount of data and files. It features a web browser base that does not require any special operation when uploading or downloading, and there is a free service (advertisement is included) and a pay service that enhances security, etc. for enterprises. When using it on campus, please avoid as much as possible sending confidential files for free using "home file service" or "data service."

It is recommended that you do a direct exchange with an encryption compatible USB or other device, or use Sophia Mail OneDrive (Office 365), strictly set the disclosure range, then send only the link to the destination.

STEP

10

Avoiding Internet Trouble (SNS, etc.)

Opportunities for individuals to disseminate information are increasing due to the popularization of services such as SNS. Careless comments are written, for example, that lead to the object of these comments becoming the target of intense criticism by large numbers of other users. This has resulted in organizations or individuals filing claims for damages.

To avoid troubles on the Internet, please take the following countermeasures.

□ When using services such as SNS, use common sense and appropriate manner in your content.

□ Recognize that it is easy to identify individuals that write. Do not advocate illegal acts or write antisocial messages.

□ Do not carelessly include personal information.

Using SNS

When sending out information using SNS for business, follow the organization's information security policy.

- □ Do not damage the brand image of the company or organization.
- □ Manage account information (ID, password, etc.) appropriately so third parties will not be hacked.
- □ Observe the terms of the service you use.
- □ Decide on a course of action for times when the service cannot be used due to things like maintenance.

STEP

11

Preventing Unauthorized Use of Online Services

Online services (news distribution, database search, etc.) are easy to use and very convenient. Online services are provided so that faculty members and students can freely browse the library at the university, but if they are used illegally, the service for the entire university may be suspended.

Please take the following actions to avoid trouble in using online services.

□ When using online services such as SNS, understand the terms of use in advance and comply with them.

□ In electronic journals and database browsing services, do not download large amounts of content at once using computer programs.

- Even for services that are said to be "free to use," the terms of use are defined between Sophia University and the service provider. Please note that the entire service may be suspended for users who do not follow the terms of service.

□ Do not borrow other people's accounts to use the service or lend your account to others.

□ Use online services with common sense and proper manners.

Examples of Sophia University Online Services

□ Sophia University Library e-Resources Access Page

Search titles of e-journals and e-books.

上智大学図書館
SOPHIA UNIVERSITY LIBRARY
e-Resources Access Page

□ Sophia University Academic Information Repository

This system aims to collect, store and preserve the academic research results and educational results of the University and make them widely available.

12

Backing Up Sensitive Information

Information (data) saved on personal computers and storage media may be lost due to malfunction, erroneous operation, virus infection, etc..

Please take the following measures to back up sensitive information.

□Periodically back up sensitive information to file server, external hard disk, etc..

Dangers of Ransomware ●

Ransomware is an illegal program that enters the user's PC, locks it, and encrypts the data, and when it secretly fulfills its purpose, it demands ransom money: "If you want a release key….” It mainly infects through targeted attack mail or when a fraudulent site is accessed, but just in case it does infect your computer, be sure to keep your data backup current.

13

Managing Important Computing Equipment

Information related to research and personal information may be recorded in personal computers (including tablets, etc.) used in research, etc.. The theft of personal computers leads to information leak.

In managing important computing equipment, please take the following measures.

□Keep personal computer and other devices under lock when not in use.

□Do not keep data on the main body of PC or other devices.

□Not saving important data on the PC itself will keep damage to a minimum in case of an incident.

STEP

14

Physically Protecting Sensitive Information

If personal computers or other devices are stolen, they can leak sensitive information such as students' personal data. Also, if you leave your computer screen open, the information displayed on the screen will be available to third parties, leading to possible information leak.

Please observe the following to physically protect sensitive information.

□ Do not leave personal computers, tablets, etc., storage media such as USBs, or documents with important information at your seat or in places like classrooms.

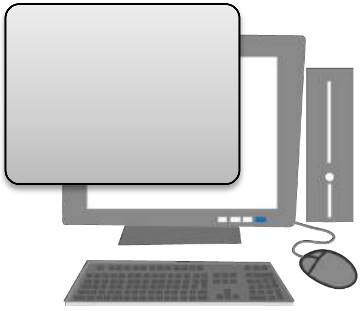
□ When leaving your desk, use a screen lock or other function to secure your computer.

☐Screen lock : 【Windows】Key ⊞ +【L】 L

☐ Desktop display : 【Windows】Key ⊞ +【D】 D

□ Do not leave documents with personal/confidential information in a place where they can be seen. Lock particularly sensitive items in a cabinet.

Using a screen privacy filter also helps keep prying eyes away!



STEP

15

Managing Sensitive Information Used Off Campus

Casually taking information off campus is a major factor causing information leak incidents. Information taken off campus can be misplaced or lost and lead to information leak.

Please observe the following with respect to taking sensitive information off campus.

□ In principle, taking personal information off campus is prohibited. To avoid even the slight possibility of theft or loss, try not to take sensitive information off campus. If you must do so, please strictly observe the following policies: Do not let the device or data out of your sight or put it on a place like a shelf. Do not participate in events such as drinking parties where alcohol is consumed.

□ When taking data off campus on a USB memory, use one that allows for encryption.

A USB memory, while convenient to carry, also has the risk of information leakage. Security-compatible USB memory has the following functions that make it safe.

･Data cannot be seen without entering a password.

･Because a virus check is executed automatically, virus infection can be prevented.

□ Avoid physically taking data off campus by using the university-approved cloud service.

In our university, OS, software and data are centrally managed on the server in the university, and the staff use thin client terminals focused on minimum functions such as input and display. This approach effectively maintains information security for terminals on which sensitive information is not stored.

□ Regularly check PC, USB memory, and other devices for personal information taken out before but no longer necessary.

※The following actions are considered taking personal information off campus:

Taking devices such as personal computers containing personal information or media such as USB off campus.

Taking paper media with personal information off campus.

STEP

16

Procedures for Disposing of Unneeded Computers

When disposing of items such as personal computers that are no longer needed or when transferring them to another person, there is the possibility of information leak from the installed hard disc, for example.

When disposing of personal computers or other devices no longer needed, please take one of the following measures:

□ Erase data using software created for this purpose (or ask a professional data-erasing company).

- Please make use of the software that can be borrowed from the ICT Office.

□ Remove the hard disk mounted on a personal computer or other device and physically destroy it.

□ When discarding medium on which personal data is recorded (CD-ROM, document, etc.), destroy it physically with a shredder or the like.

The ICT Office has started a safe disposal service for ICT equipment (PCs, servers, etc.). Please consult with the ICT Office for disposal of equipment on which important data such as students’ personal information is stored.

Social Engineering･･･

Social engineering is a method of stealing important information such as passwords necessary to infiltrate a network without using information communication technology, taking advantage of human psychological gaps and behavioral mistakes.

Example
Dumpster diving (trashing)

Countermeasures:
Have professional disposal company dispose of garbage.
Strengthen office entry/exit management to prevent unauthorized outsiders from entering the company illegally.
Take full precautions in disposing of documents.

STEP

16

Proper Software Management

Since software is a copyrighted work, copying or distributing it illegally makes one subject to criminal penalty and damages compensation.

Please manage software properly, observing the following:

□ Confirm the content of the software license (usage rights, etc.).

□ Do not copy software illegally.

□ Use software as stipulated in the contract.

Free Microsoft Office Use●

Faculty, staff, and students at Sophia University and Sophia Social Welfare College can download and use Microsoft Office for free while they are employed by or enrolled at Sophia.

□ Microsoft Office is for Sophia University / Sophia University Junior College Division / Sophia School of Social Welfare faculty, staff, and students who have a Sophia Mail account.

□ Upon graduation, withdrawal from school, or leaving Sophia, the account will be cancelled.

□ Microsoft Office can be installed on up to five computers or devices, including ones used at home.

※ For details: see URL

https://ccweb.cc.sophia.ac.jp/userguide/service/sv_11/

STEP

17

Server Room Management

In order to maintain information security, before installing a server or other equipment for use in research, etc., confirm that the room is secure and able to be locked. In places where many people go in and out, the risk of theft or improper server operation increases, along with possibility that information may be stolen.

Please manage the server room as follows:

□ Take precautions for locking the room in which the server is installed.

□ Use a system such as control slips for those entering and exiting the room in which the server is installed.

Room Entering/Exiting Security

- □ Follow procedures for locking and unlocking offices.
- □ Keep a record of those entering and exiting the room (in a ledger, etc.).
- □ Issue and require employees to carry identification cards.
- □ Always keep a lookout for suspicious persons in places where there is heavy traffic.
- □ Restrict entry and exit by security card, etc..
- □ Place a guard at the entrance and set up surveillance cameras.
- □ Introduce a more robust security system using technology such as biometrics.

Resources for ICT Security

Security updates
Information-Technology Promotion Agency,
Independent Administrative Institution
(https://www.ipa.go.jp/security/personal/)

Security alerts
JPCERT Coordination Center
(https://www.jpcert.or.jp/)

Copyright information
Public Interest Corporation Copyright Information Center
(http://www.cric.or.jp/)

Campus ICT Security Rules and Resources

· Sophia University Information Security Basic Policy
· Sophia University Information System Security Regulations
(https://kitei.cl.sophia.ac.jp/doc/suallstaffs/listall.html#)

Systems Usage Guide
Sophia University ICT Office (Media Center)
(https://ccweb.cc.sophia.ac.jp/userguide/)

In case of an ICT security incident

In the case of a possible ICT security incident such as a personal computer, USB, or other item being lost or a computer being infected with a computer virus, promptly contact the General Affairs Group or the ICT Office (Media Center).

Loss of personal computer or USB memory
Department: General Affairs Group
Contact: 03-3238-3172 Ext. 3172

Technical inquiries
Department: ICT Office
Contact: 03-3238-3101 Ext. 3101 or 4473

For safe disposal of ICT equipment

The ICT Office has started a safe disposal service for ICT equipment (PCs, servers, etc.). Please consult with the ICT Office for disposal of equipment on which important data such as students' personal information is stored.

Department: ICT Office
Contact: 03-3238-3101 Ext. 3101 or 4473

Sources

- ◘ Ministry of Internal Affairs "ICT Security Site for Citizens"
(http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html)
- ◘ Independent Administrative Agency Information Processing Center Security Center (IPA) "Minimal Information Security Measures for Businesses and Organizations + 1
(https://www.ipa.go.jp/security/keihatsu/shiori/management/01_guidebook.pdf)